LAPORAN PRAKTIKUM

KEAMANAN INFORMASI 1

PERTEMUAN 3

(Analisis Malware)

DISUSUN OLEH
Indah Sekar Ningrum (21/478139/SV/19241)

SARJANA TERAPAN TEKNOLOGI REKAYASA INTERNET

DEPARTEMEN TEKNIK ELEKTRO DAN INFORMATIKA

SEKOLAH VOKASI

UNIVERSITAS GADJAH MADA

YOGYAKARTA

2023

A. LATAR BELAKANG

1. Virus

Virus adalah jenis malware yang menggandakan diri dengan memodifikasi program komputer lain dan memasukkan kode mereka sendiri ketika dieksekusi. Ketika replikasi ini berhasil, area yang terkena kemudian dikatakan terinfeksi.

Virus menggunakan rekayasa sosial dan mengeksploitasi kerentanan untuk menginfeksi sistem dan menyebarkan virus. Sistem operasi Microsoft Windows dan Mac adalah target dari sebagian besar virus yang sering menggunakan strategi anti-deteksi kompleks untuk menghindari perangkat lunak antivirus.

Virus dibuat untuk menghasilkan keuntungan (mis. ransomware), mengirim pesan, hiburan pribadi, menunjukkan adanya kerentanan , sabotase dan penolakan layanan , atau untuk sekadar menjelajahi masalah keamanan dunia maya , kehidupan buatan, dan algoritme evolusioner.

Virus komputer menyebabkan kerusakan ekonomi senilai miliaran dolar dengan menyebabkan kegagalan sistem, pemborosan sumber daya, merusak data, meningkatkan biaya pemeliharaan, mencatat penekanan tombol, dan mencuri informasi pribadi (mis. nomor kartu kredit).

2. Worm

Worm adalah program malware yang mereplikasi diri sendiri yang tujuan utamanya adalah menginfeksi komputer lain dengan menggandakan dirinya sendiri sambil tetap aktif pada sistem yang terinfeksi.

Seringkali, worm menggunakan jaringan komputer untuk menyebar, bergantung pada kerentanan atau kegagalan keamanan pada komputer target untuk mengaksesnya. Cacing hampir selalu menyebabkan setidaknya beberapa kerusakan pada jaringan, meskipun hanya dengan menghabiskan bandwidth. Ini berbeda dengan virus yang hampir selalu merusak atau mengubah file di komputer korban.

WannaCry adalah contoh terkenal dari ransomware cryptoworm yang menyebar tanpa tindakan pengguna dengan mengeksploitasi kerentanan EternalBlue.

Sementara banyak worm dirancang untuk hanya menyebar dan tidak mengubah sistem yang mereka lewati, bahkan worm bebas muatan dapat menyebabkan gangguan besar. Worm Morris dan Mydoom menyebabkan gangguan besar dengan meningkatkan lalu lintas jaringan meskipun sifatnya jinak.

3. Trojan horse

Trojan horse atau trojan adalah malware apa pun yang menyesatkan pengguna tentang niat sebenarnya dengan berpura-pura menjadi program yang sah. Istilah ini berasal dari cerita Yunani Kuno tentang Kuda Troya yang menipu yang menyebabkan jatuhnya kota Troy.

Trojan umumnya disebarkan dengan social engineering seperti phishing. Misalnya, pengguna mungkin tertipu untuk menjalankan lampiran email yang disamarkan agar terlihat asli (misalnya spreadsheet Excel). Setelah file yang dapat dieksekusi dibuka, trojan diinstal.

Meskipun muatan trojan bisa berupa apa saja, sebagian besar bertindak sebagai pintu belakang yang memberi penyerang akses tidak sah ke komputer yang terinfeksi. Trojan dapat memberikan akses ke informasi pribadi seperti aktivitas

internet, kredensial login perbankan, kata sandi, atau informasi identitas pribadi. Serangan ransomware juga dilakukan dengan menggunakan trojan.

Tidak seperti virus komputer dan worm, trojan umumnya tidak mencoba menyuntikkan kode berbahaya ke file lain atau menyebarkan dirinya sendiri.

4. Rootkits

Rootkit adalah kumpulan malware yang dirancang untuk memberikan akses tidak sah ke komputer atau area perangkat lunaknya dan seringkali menutupi keberadaannya atau keberadaan perangkat lunak lain.

Instalasi rootkit dapat dilakukan secara otomatis atau penyerang dapat menginstalnya dengan akses administrator. Akses dapat diperoleh sebagai akibat dari serangan langsung pada sistem, seperti mengeksploitasi kerentanan , meretas kata sandi, atau phishing. Deteksi rootkit sulit dilakukan karena dapat menumbangkan program antivirus yang dimaksudkan untuk menemukannya. Metode deteksi termasuk menggunakan sistem operasi tepercaya, metode perilaku, pemindaian tanda tangan, pemindaian perbedaan, dan analisis dump memori.

Penghapusan rootkit bisa menjadi rumit atau praktis tidak mungkin, terutama ketika rootkit berada di dalam kernel. Rootkit firmware mungkin memerlukan penggantian perangkat keras atau peralatan khusus.

5. Ransomware

Ransomware adalah bentuk malware, yang dirancang untuk menolak akses ke sistem komputer atau data hingga uang tebusan dibayarkan. Ransomware menyebar melalui email phishing, malvertising, mengunjungi situs web yang terinfeksi, atau dengan mengeksploitasi kerentanan.

Serangan ransomware menyebabkan downtime, kebocoran data, pencurian kekayaan intelektual, dan pelanggaran data. Jumlah pembayaran tebusan berkisar dari beberapa ratus hingga ratusan ribu dolar. Dapat dibayar dalam mata uang kripto seperti Bitcoin.

6. Keylogger

Keylogger, keystroke logger, atau pemantauan sistem adalah jenis malware yang digunakan untuk memantau dan merekam setiap penekanan tombol yang diketik pada keyboard komputer tertentu. Keyloggers juga tersedia untuk smartphone.

Keylogger menyimpan informasi yang dikumpulkan dan mengirimkannya ke penyerang yang kemudian dapat mengekstrak informasi sensitif seperti kredensial login dan detail kartu kredit.

7. Grayware

Istilah grayware diciptakan pada bulan September 2004 dan menjelaskan aplikasi atau file yang tidak diinginkan yang bukan merupakan malware tetapi memperburuk kinerja komputer dan dapat menyebabkan risiko keamanan dunia maya.

Minimal, greyware berperilaku mengganggu atau tidak diinginkan dan paling buruk, memantau sistem dan menelepon ke rumah dengan informasi.

Grayware menyinggung adware dan spyware. Kabar baiknya adalah sebagian besar perangkat lunak antivirus dapat mendeteksi program yang mungkin tidak diinginkan dan menawarkan untuk menghapusnya.

Adware dan spyware umumnya mudah dihapus karena tidak sejahat jenis malware lainnya.

Kekhawatiran yang lebih besar adalah mekanisme yang digunakan grayware untuk mendapatkan akses ke komputer, baik itu rekayasa sosial , perangkat lunak yang belum ditambal, atau kerentanan lainnya . Bentuk malware lain seperti ransomware dapat menggunakan metode yang sama untuk mendapatkan akses.

Gunakan kehadiran adware sebagai peringatan bahwa perangkat atau pengguna memiliki kelemahan yang harus diperbaiki.

8. Fileless Malware

Malware tanpa file adalah jenis malware yang menggunakan program resmi untuk menginfeksi komputer. Tidak seperti infeksi malware lainnya, itu tidak bergantung pada file dan tidak meninggalkan jejak, sehingga sulit untuk dideteksi dan dihapus oleh perangkat lunak anti-malware. Itu ada secara eksklusif sebagai artefak berbasis memori komputer yaitu di RAM.

Malware tanpa file muncul pada tahun 2017 sebagai ancaman dunia maya utama tetapi telah ada untuk sementara waktu. Frodo, Number of the Beast, dan Dark Avenger semuanya adalah serangan awal malware tanpa file. Baru-baru ini, Komite Nasional Demokrat dan pelanggaran Equifax menjadi korban serangan malware tanpa file.

Malware tanpa file tidak menulis bagian apa pun dari aktivitasnya ke hard drive komputer sehingga tahan terhadap strategi forensik anti-komputer yang ada untuk memasukkan daftar putih berbasis file, deteksi tanda tangan, verifikasi perangkat keras, analisis pola, atau stempel waktu.

Ini menyisakan sangat sedikit bukti yang dapat digunakan oleh penyelidik forensik digital untuk mengidentifikasi aktivitas tidak sah. Yang mengatakan, karena dirancang untuk bekerja dalam memori, umumnya hanya ada sampai sistem di-reboot.

9. Adware

Adware adalah jenis perangkat abu-abu yang dirancang untuk memasang iklan di layar Anda, seringkali di browser web atau sembulan.

Biasanya itu membedakan dirinya sebagai yang sah atau mendukung program lain untuk mengelabui Anda agar menginstalnya di komputer, tablet, atau ponsel cerdas Anda.

Adware adalah salah satu bentuk malware yang paling menguntungkan, paling tidak berbahaya, dan menjadi semakin populer di perangkat seluler. Adware menghasilkan pendapatan dengan menampilkan iklan secara otomatis kepada pengguna perangkat lunak.

10. Malvertising

Malvertising, sebuah portmanteau dari iklan berbahaya, adalah penggunaan iklan untuk menyebarkan malware. Ini biasanya melibatkan menyuntikkan iklan berbahaya atau berisi malware ke dalam jaringan iklan dan halaman web yang sah.

Periklanan adalah cara yang bagus untuk menyebarkan malware karena upaya yang signifikan dimasukkan ke dalam iklan untuk membuatnya menarik pengguna untuk menjual atau mengiklankan produk.

Malvertising juga mendapat manfaat dari reputasi situs tempatnya ditempatkan, seperti situs web berita terkenal dan bereputasi baik.

11. Spyware

Spyware adalah malware yang mengumpulkan informasi tentang seseorang atau organisasi, terkadang tanpa sepengetahuan mereka, dan mengirimkan informasi tersebut ke penyerang tanpa persetujuan korban.

Spyware biasanya bertujuan untuk melacak dan menjual data penggunaan internet Anda, mengambil informasi kartu kredit atau rekening bank Anda, atau mencuri informasi identitas pribadi (PII).

Beberapa jenis spyware dapat menginstal perangkat lunak tambahan dan mengubah pengaturan di perangkat Anda. Spyware biasanya mudah dihapus karena tidak sejahat jenis malware lainnya.

12. Bot dan Botnet

Bot adalah komputer yang terinfeksi malware yang memungkinkannya dikendalikan dari jarak jauh oleh penyerang.

Bot (atau komputer zombie) kemudian dapat digunakan untuk meluncurkan lebih banyak serangan dunia maya atau menjadi bagian dari botnet (kumpulan bot).

Botnet adalah metode populer untuk serangan distributed denial of service (DDoS), menyebarkan ransomware, keylogging, dan menyebarkan jenis malware lainnya.

13. Backdoor

Backdoor adalah metode rahasia untuk melewati otentikasi atau enkripsi normal di komputer, produk, perangkat yang disematkan (misalnya router) atau bagian lain dari komputer.

Backdoor biasanya digunakan untuk mengamankan akses jarak jauh ke komputer atau mendapatkan akses ke file terenkripsi.

Dari sana, dapat digunakan untuk mengakses, merusak, menghapus, atau mentransfer data sensitif.

Backdoors dapat berupa bagian tersembunyi dari sebuah program (kuda trojan), program atau kode terpisah dalam firmware dan sistem operasi.

Selanjutnya, backdoors dapat dibuat atau diketahui secara luas. Banyak backdoor memiliki kasus penggunaan yang sah seperti pabrikan yang membutuhkan cara untuk mengatur ulang kata sandi pengguna.

14. Browser Hijacker

Browser hijacker atau hijackware mengubah perilaku peramban web dengan mengirim pengguna ke laman baru, mengubah beranda, memasang bilah alat yang

tidak diinginkan, menampilkan iklan yang tidak diinginkan, atau mengarahkan pengguna ke situs web lain.

15. Crimeware

    Crimeware adalah kelas malware yang dirancang untuk mengotomatiskan kejahatan dunia maya.

    Ini dirancang untuk melakukan pencurian identitas melalui rekayasa sosial atau sembunyi-sembunyi untuk mengakses akun keuangan dan ritel korban untuk mencuri dana atau melakukan transaksi tidak sah. Atau, mungkin mencuri informasi rahasia atau sensitif sebagai bagian dari spionase perusahaan.

16. Malicious Mobile Apps

    Aplikasi berbahaya dapat mencuri informasi pengguna, mencoba memeras pengguna, mendapatkan akses ke jaringan perusahaan, memaksa pengguna untuk melihat iklan yang tidak diinginkan, atau memasang pintu belakang di perangkat.

17. RAM Scraper

    RAM Scraper RAM adalah jenis malware yang memanen data yang disimpan sementara di memori atau RAM. Jenis malware ini sering menargetkan sistem point-of-sale (POS) seperti mesin kasir karena mereka dapat menyimpan nomor kartu kredit yang tidak terenkripsi untuk waktu yang singkat sebelum mengenkripsinya kemudian meneruskannya ke back-end.

18. Rogue Security Software

    Rogue Security Software menipu pengguna untuk berpikir bahwa sistem mereka memiliki masalah keamanan seperti virus dan membujuk mereka untuk membayar agar menghapusnya. Pada kenyataannya, perangkat lunak keamanan palsu adalah malware yang perlu dihapus.

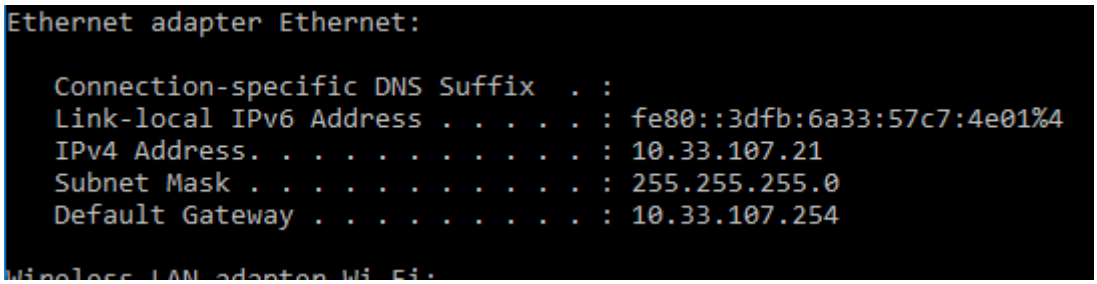
19. Cryptojacking

    Cryptojacking adalah jenis malware yang menggunakan daya komputasi korban untuk menambang cryptocurrency.

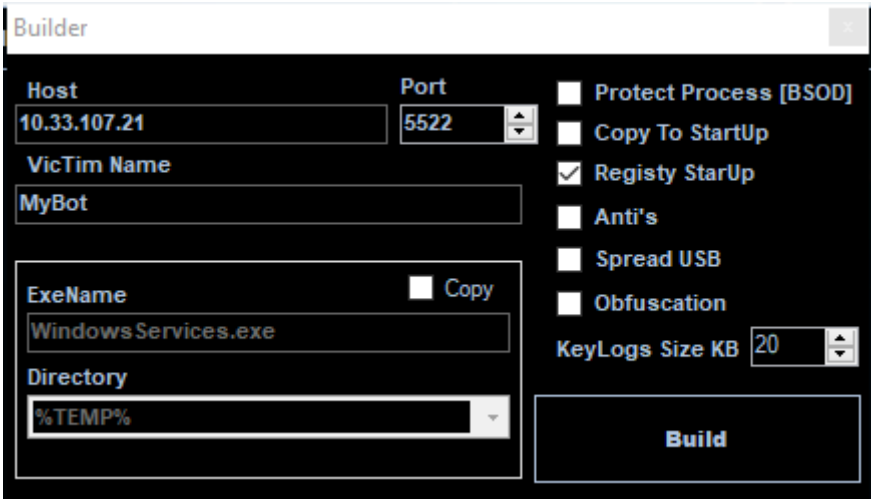
B. LANGKAH - LANGKAH

1. Download dan ekstrak aplikasi NJRAT kemudian run aplikasi NJRAT pada komputer host.
   https://github.com/adarift/njRAT/releases/tag/v0.7D
   Masukkan port yang ingin digunakan 5520

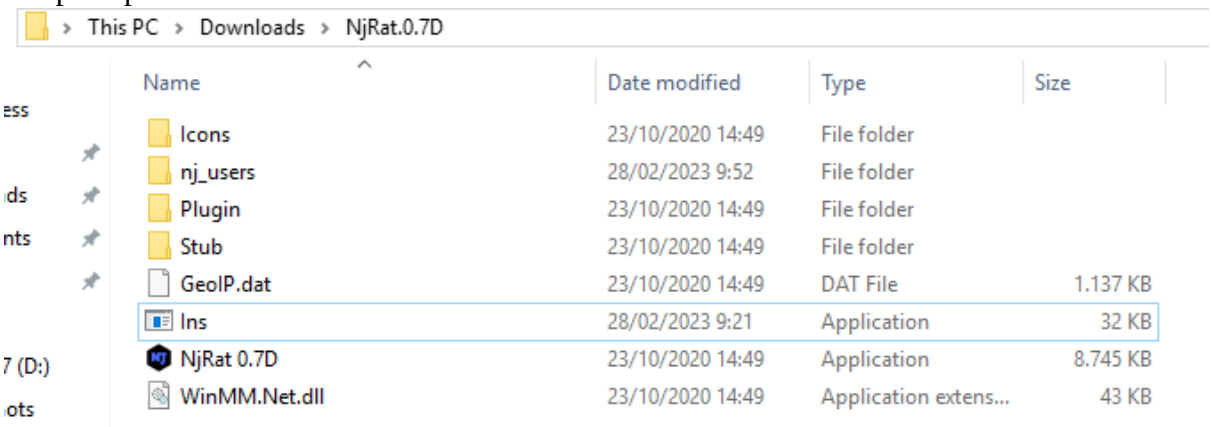
2. Sebelumnya, cek IP Address milik host terlebih dahulu. IP ini nantinya akan digunakan oleh NJRAT, dan pastikan juga komputer victim berada pada satu jaringan. Perintah ipconfig pada Command Prompt.



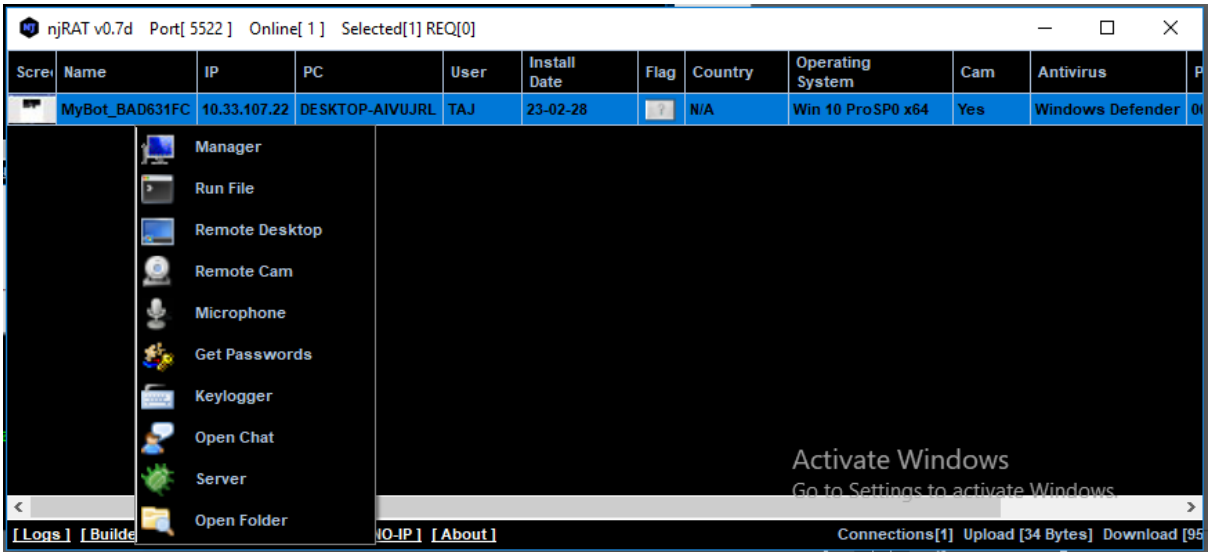
3. Buat aplikasi yang akan dipasang pada komputer victim. Masukkan IP Address host pada kolom host dan port yang sesuai dengan yang kita tentukan tadi pada awal membuka aplikasi NJRAT agar dapat diakses oleh komputer nanti, kemudian klik tombol build.



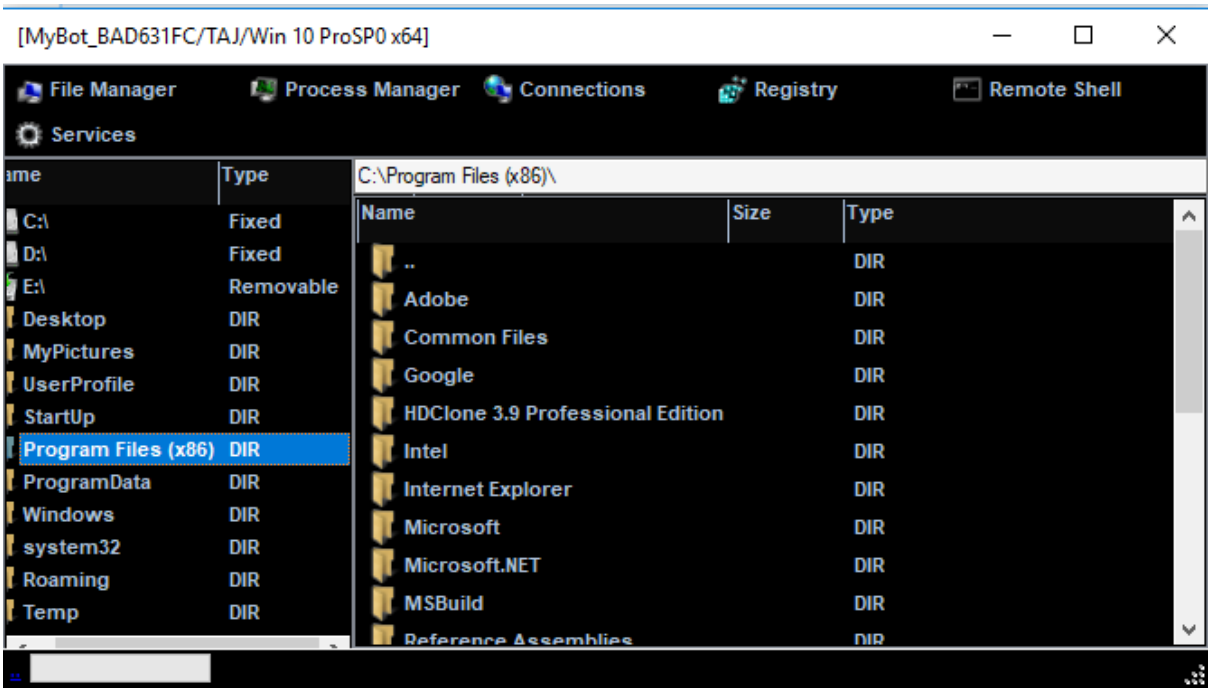
4. Simpan aplikasi hasil build.



5. Kemudian, copykan aplikasi Ins.exe yang sudah telah kita buat ke dalam komputer victim. Kemudian, pada komputer victim jalankan aplikasi tersebut. Ketika sudah terpasang pada komputer victim, NJRAT pada host akan mendeteksi komputer victim.

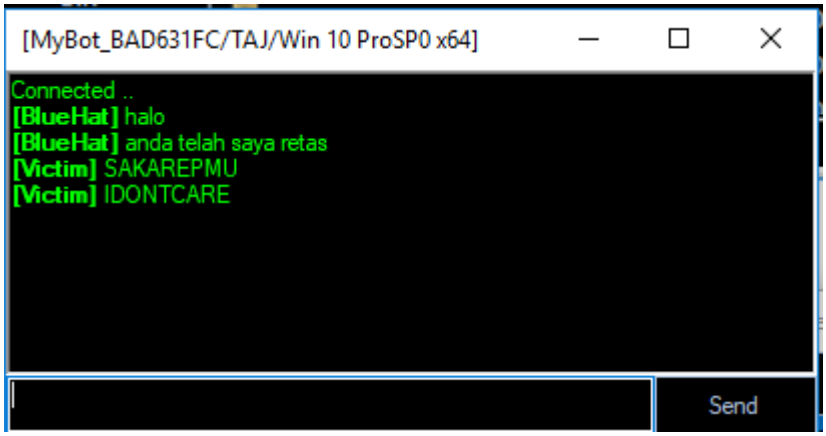


6. Klik kanan pada komputer yang aktif maka akan muncul beberapa pilihan menu, pilih menu manager agar dapat melihat seluruh isi file manager yang ada pada komputer victim.

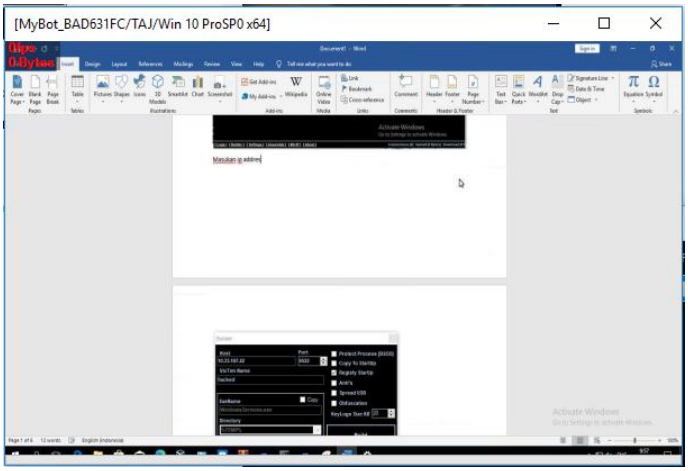


7. Pada menu remote cam maka akan membuka webcam yang ada di komputer victim dan dapat melihat segala aktivitas yang dilakukan oleh victim

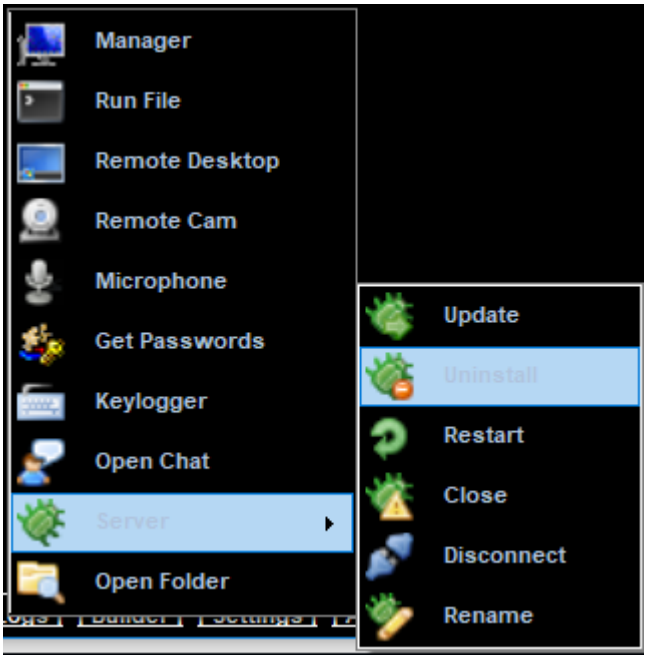
8. Pada pilihan chat message, kita dapat mengirimkan pesan ke layar desktop komputer victim, dan user komputer dapat melakukan balasan tanpa bisa menutup chat



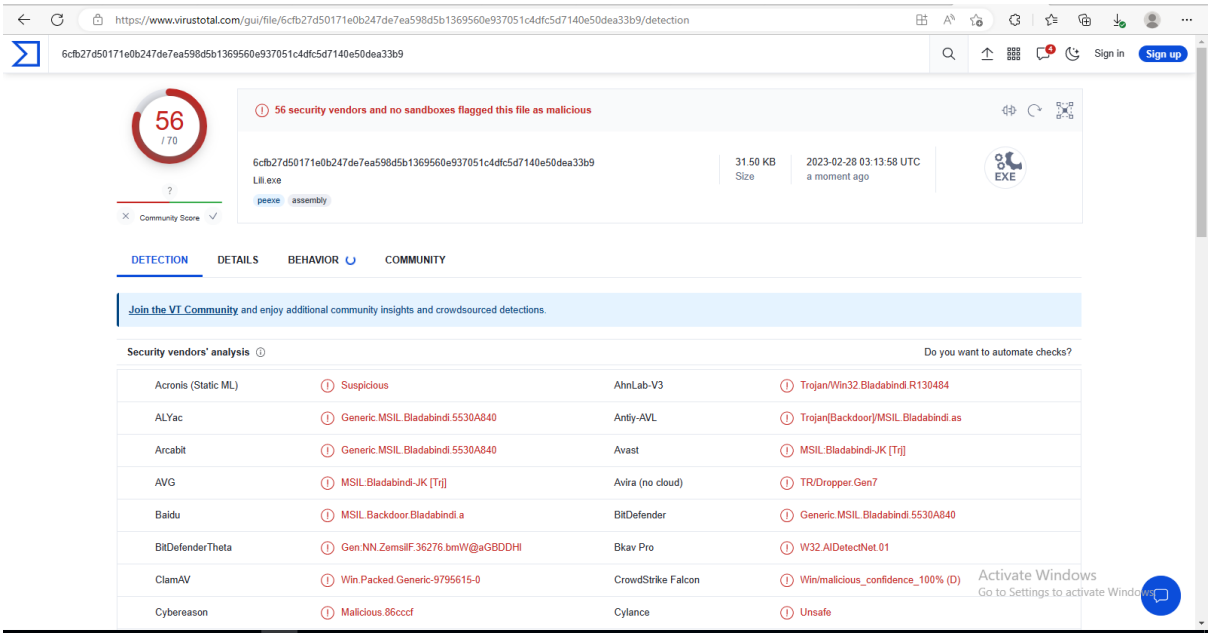
9. Dekstop monitor



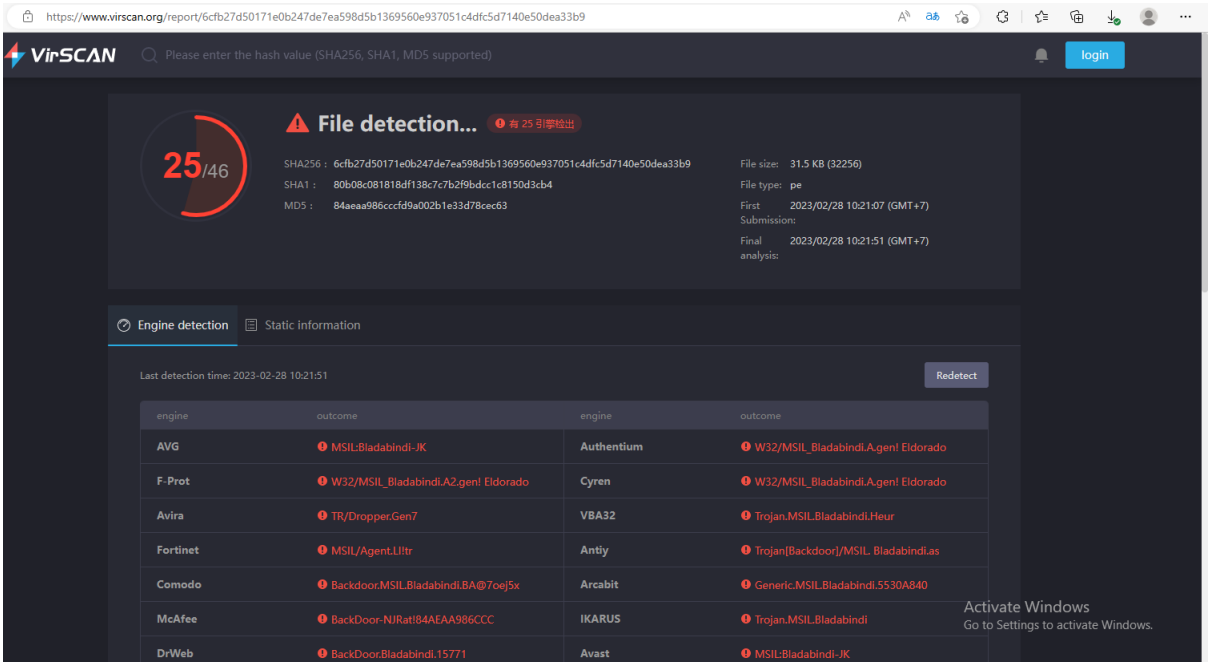
10. Keluar



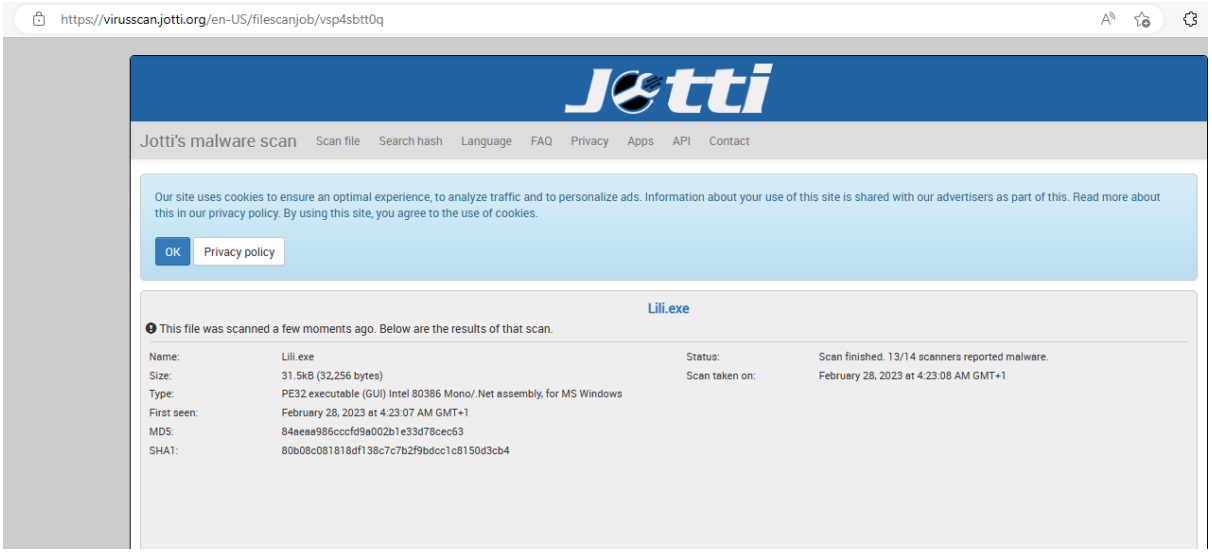
11. VirusTotal



12. VirSCAN



13. Jotti



14. Polyswarm